ABSTRAKSI

Kebutuhan akan informasi yang *mobile* juga menjadi latar belakang bagi perkembangan teknologi proteksi komunikasi data. Tidak jarang ditemui adanya perilaku kriminal yang mencoba masuk ke celah-celah komunikasi data ini. Ketika membicarakan tentang keamanan data, maka salah satu solusi yang terpikir adalah kriptografi. Kriptografi adalah suatu cabang ilmu matematika yang memanfaatkan proses komputasi untuk mengacak data yang akan dikirimkan. Enkripsi adalah sebuah proses data *encoding* untuk mencegah pihak yang tidak berwenang melihat atau memodifikasinya.

Dalam tugas akhir ini diimplementasikan tiga algoritma yang digunakan dalam kriptografi, antara lain *hash function* dengan algoritma MD5 dan SHA1, serta algoritma kriptografi simetrik, yaitu RC4. Algoritma-algoritma tersebut adalah solusi yang ditawarkan dalam dunia kriptografi dan sudah umum digunakan dalam jaringan *internet*. Semua algoritma yang diimplementasikan diadaptasi kedalam sistem yang menggunakan *platform* J2ME.

Sistem yang telah diimplementasikan dapat berjalan baik pada *emulator* J2ME Wireless Toolkit. Analisa terhadap subsistem *security* dilakukan berdasarkan beberapa parameter yaitu panjang data *output*, penggunaan *memory*, waktu proses, distribusi frekuensi kemunculan karakter, variansi distribusi, *avallanche effect* untuk algoritma RC4, dan waktu untuk melakukan *brute force attack* pada algoritma RC4.

Dari hasil analisa terhadap parameter-parameter diatas dibandingkan performansi yang lebih baik antara algoritma *hash function* MD5 dan SHA1. Dari proses tersebut diperoleh bahwa algoritma SHA1 memiliki keunggulan pada parameter panjang data *output*, waktu proses dengan kombinasi algoritma RC4, distribusi frekuensi, variansi, dan waktu *brute force attack*. Algoritma MD5 memiliki keunggulan pada parameter penggunaan *memory*, dan waktu proses tanpa kombinasi algoritma RC4. Maka secara umum algoritma SHA1 memiliki performansi yang lebih baik daripada MD5.